Zerona

サイバー攻撃からPCを守る マルウェア対策ソフトウェア
InfoTrace PLUS シリーズ ゼロナ

従来のセキュリティ対策だけでは防御できない！

- パターンファイルでは新種マルウェアを検知できない！
- ゼロデイ脆弱性は、パッチ適用でも完全に防御できない！
- 攻撃技術が進化し、従来の検知手法をすり抜ける！

Zeronaは 高度化するサイバー攻撃から徹底防御！

多層構造の検知エンジン

パターンファイルに依存せず、高度な攻撃や新種マルウェアからPCを徹底防御する各種エンジンを搭載。

脆弱性攻撃を阻止

ゼロデイ脆弱性を突く攻撃もブロック！高度な標的型サイバー攻撃の第一歩をエンドポイントで阻止します。

大規模環境への対応

設定・バージョンアップの配信は、プッシュ型で計画実行が可能。Zeronaの防御機能を最大限に引き出す各種の管理機能を実装。

Zerona

圧倒的な検知能力でサイバー攻撃・マルウェアから防御

サイバー攻撃で狙われるエンドポイントでの脆弱性攻撃・マルウェア侵入を徹底ブロック。従来対策をすり抜ける昨今の攻撃にも対応した各種の振る舞い検知技術を搭載し、エンドポイントでの防御力を強化します。

検知・ブロック

コード実行型攻撃の検知・防御 ZDP

- 既知・未知の脆弱性を狙うコード実行型攻撃を徹底検知・防御
- 従来の検知機能をバイパスする進化した攻撃※にも対応
- メール添付される文書ファイル等での標的型攻撃もブロック
- Web閲覧で感染するDrive-by-download型にも対応

※ Return-into-libcやROPなど、近年の高度な攻撃手法にも対応。

マルウェア静的分析 Static

- あらゆるマルウェア（ウイルス、トロイの木馬、ボット、ワーム）を、高度な静的分析ロジックで検知
- パターンに依存しないため、新種マルウェアも検知可能

仮想環境上での振る舞い検知 Sandbox

- 疑わしいプログラムを閉鎖された仮想環境で実施し、動作していなければ判定できないマルウェアを検出
- 実環境に影響を及ぼすことなく、より確実な検知を実現
- 近年のマルウェアが持つサンドボックス回避技術にも対応

実行プロセスの動作を監視 HIPS

- 疑わしいプロセスを監視し、怪しい挙動を検知・ブロック
- 他プロセスへの侵入、キーロガーやバックドアを洗い出し、情報漏えいにつながるアクションを阻止

機械学習エンジンでの挙動監視 Machine Learning

- マルウェア・正常ソフトウェアを機械学習させ抽出された、マルウェアの傾向・特徴をエンジンとして実装
- 未知のマルウェアによる悪意のある挙動を検知・ブロック

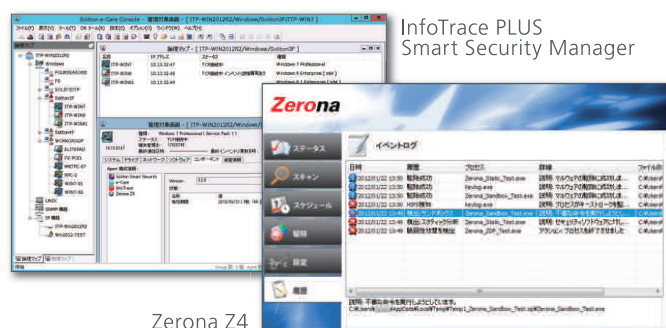
運用・管理

端末への負荷がかからない設計

- パターンファイルに依存せず、端末に負荷がかからない設計
- 日々のパターンファイル更新や頻繁なフルスキャンも不要
- インターネット接続が無い環境でも利用可能
- 主要ウイルス対策ソフトとの共存も確認

統合管理

- 大規模環境に対応した、Zeronaの管理・運用機能
- 検知ポリシーやホワイトリスト、バージョンアップのプッシュ配信・計画配信
- オフライン端末への配慮（ポリシーやライセンスを投入した状態での導入）
- マルウェア検知時のアラートメール・任意のアプリケーション実行
- ライセンス期限の事前通知や該当端末の検索による期限切れの防止
- パッチ適用も可能なファイル配信機能
- 管理サーバーのバックアップ・リストアツールなども標準提供

InfoTrace PLUS Smart Security Manager

Zerona Z4

駆除・対応

駆除・修復

- 次々に新しいマルウェアをダウンロードする「シーケンシャル・マルウェア」に対応、変更履歴からマルウェア徹底駆除・システム修復を実施
- 検知された疑わしいファイルの取得（検体確保）や駆除は、必要に応じて管理者から実行可能

包括的なインシデント対応

- Zerona PLUSでは、脆弱性攻撃防御やマルウェア対策に加え、マルウェアの侵入経緯や被害範囲の把握に役立つPC操作ログ機能を提供カーネルレベルの高精度PC操作ログは内部不正対策としても活用可能
- NetAttest BigDataを利用すれば、Zeronaの検知イベントとInfoTrace PLUSのPC操作ログのスピーディな統合分析が可能

モデル

モデル	ZDP	Static	Sandbox	HIPS	Machine Learning	PC操作ログ	機能
Zerona	●	●	●	●	●	—	脆弱性攻撃の防御と振る舞い検知を含む各種マルウェア対策を搭載
Zerona PLUS	●	●	●	●	●	●	Zeronaに、高精度PC操作ログ機能を追加した強化モデル

※ ZeronaはZerona Z4を表します。
※ Zerona PLUSは、インシデント発生時にマルウェアの侵入経緯や被害範囲の把握、内部不正対策にも活用できる高精度なPC操作ログを追加した強化モデルです。

Zerona/Zerona PLUS 動作環境（エージェント）

OS	Windows Vista（32bit）、Windows 7（32bit/64bit）、Windows 8/8.1（32bit/64bit）

InfoTrace PLUS Smart Security Manager 動作環境（管理サーバー）

OS	Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2

※ サービスパック、必要ハードウェア環境、サイジングなどの詳細はお問い合わせください。
※ 仮想環境でもご利用いただけます。詳細はお問い合わせください。
※ 本製品は、株式会社FFRIの特許技術を含む各種マルウェア対策テクノロジーを使用しています。

⚠ 安全に関するご注意	正しく安全にお使いいただくために、ご使用の前に必ず「取扱説明書」をお読みください。

Soliton®
株式会社ソリトンシステムズ　http://www.soliton.co.jp/
〒160-0022　東京都新宿区新宿 2-4-3
TEL 03-5360-3811　netsales@soliton.co.jp
大阪営業所 06-6821-6777　福岡営業所 092-263-0400
名古屋営業所 052-963-9700　東北営業所 022-716-0766
札幌営業所 011-242-6111

このカタログは 2015 年 7 月現在のものです。仕様、デザインは予告なく変更することがあります。　Zerona-1507A